UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA
Criminal No. 09-CR-242 MJD/FLN

UNITED STATES OF AMERICA,

Plaintiff,

v.

MAHAMUD SAID OMAR,

Defendant.

GOVERNMENT'S UNCLASSIFIED MEMORANDUM IN OPPOSITION TO THE DEFENDANT'S MOTION RELATING TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

I. INTRODUCTION

The Government is filing this classified memorandum in opposition to the sealed Motion for Disclosure and Review of all FISA Applications, Review of Rulings Made by the FISC, and Suppression of all FISA-Derived Evidence ("the FISA Motion"), relating to the Foreign Intelligence Surveillance Act, as amended ("FISA"),[1] filed by the defendant, Mahamud Said Omar ("the defendant"). The FISA Motion seeks: (1) the Court's review of all applications for electronic surveillance of the defendant or any third-party target in relation to which the defendant was intercepted; (2) disclosure to the defendant of such applications and any related orders following the Court's review of such documents; (3) a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978); and (4) suppression of all information and evidence obtained or derived from electronic surveillance and physical search conducted pursuant to FISA, including the fruits of any evidence developed from such surveillance or search. (Def. FISA Mot. at 1.)

[CLASSIFIED MATERIAL REDACTED]

A. BACKGROUND

On August 20, 2009, a federal grand jury sitting in the District of Minnesota returned a five-count indictment charging the defendant with one count of conspiracy to provide material support to terrorists, in violation of 18 U.S.C. § 2339A; one count of providing material support

[1] The provisions of FISA that deal with electronic surveillance are located at 50 U.S.C. §§ 1801-1812; those that deal with physical searches are located at 50 U.S.C. §§ 1821-1829. The two sets of provisions are in many respects parallel and almost identical. Citations herein are generally to the two sets of provisions in parallel, with the first citation being to the relevant electronic surveillance provision, and the second citation being to the relevant physical search

to terrorists, in violation of 18 U.S.C. §§ 2339A and 2; one count of conspiracy to provide material support to a foreign terrorist organization, in violation of 18 U.S.C. § 2339B(a)(1); one count of providing material support to a foreign terrorist organization, in violation of 18 U.S.C. §§ 2339B(a)(1) and 2; and one count of conspiracy to kill, kidnap, maim, and injure, in violation of 18 U.S.C. § 956. The indictment was unsealed on November 23, 2009.

[CLASSIFIED MATERIAL REDACTED]

On August 16, 2011, pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), the Government provided written notice to this Court and to the defendant that the United States "intends to offer into evidence, or otherwise use or disclose in any proceedings in the above-captioned matter, information obtained or derived from electronic surveillance and/or physical search conducted pursuant to the Foreign Intelligence Surveillance Act of 1978." (*See* Notice of Intent to Use FISA Information, Docket No. 27, *United States v. Omar*, No. 09-CR-242 (MJD/FLN) (D. Minn. 2011)).

On February 13, 2011, the defendant filed the FISA Motion under seal and moved for the disclosure of certain FISA materials and the suppression of FISA-obtained or –derived information and evidence. In so moving, the defendant relies upon FISA, the First, Fourth, Fifth, and Sixth Amendments to the U.S. Constitution, and *Brady v. Maryland*, 373 U.S. 83 (1963), and raises the following arguments: (1) that FISA is unconstitutional as written and as applied to the FISA collection at issue; (2) that the FISA applications at issue fail to make the requisite showings to permit collection under FISA, in that they do not demonstrate that a

---

provision.

significant purpose of the collections at issue was to obtain foreign intelligence and because probable cause was lacking to authorize such collections; (3) that the certifications required by 18 U.S.C. § 1804(a)(6) were clearly erroneous; and (4) that the applications at issue contain false statements in violation of *Franks*. (*See generally* Def. FISA Motion.) The defendant also contends that the Government may have failed to comply with the dates of authorized collection, and noted for the Court that the defendant was unable to properly attack any collection under FISA without reviewing the applications at issue. (*See generally id.*)

[CLASSIFIED MATERIAL REDACTED]

The Government's response and the supporting FISA materials are submitted to oppose the defendant's FISA Motion and aid the Court in its statutorily mandated *in camera, ex parte* review of the FISA materials, required by 50 U.S.C. §§ 1806(f) and 1825(g), where, as here, the Attorney General has filed a Declaration and Claim of Privilege. These materials are also filed to support the United States' request, pursuant to FISA, that this Court do the following: (1) find that the FISA collection at issue was lawfully authorized and conducted; and (2) order that none of the classified documents, nor any of the classified information contained therein, be disclosed to the defense, and instead, that they be maintained by the United States under seal. As the discussion below will demonstrate, all of the defendant's arguments are without merit, and his requests for relief should be denied.

B. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

II. THE FISA PROCESS

A. OVERVIEW OF FISA

Enacted in 1978, and subsequently amended, FISA authorizes the Chief Justice of the United States to designate eleven United States District Judges to sit as judges of the FISC. 50 U.S.C. § 1803(a)(1). The FISC judges are empowered to consider *ex parte* applications submitted by the Executive Branch for electronic surveillance and physical searches when a significant purpose of the application is to obtain foreign intelligence information, as defined by FISA. Rulings of the FISC are subject to review by the Foreign Intelligence Surveillance Court of Review ("FISC of Review"), which is the specialized federal appellate court composed of three U.S. District or Circuit Judges designated by the Chief Justice that Congress established to hear appeals from the FISC. 50 U.S.C. § 1803(b). As discussed below, a U.S. District Court also has jurisdiction to determine the legality of electronic surveillance and physical searches authorized by the FISC when the fruits of that intelligence collection are used against an "aggrieved person."[2] *See* 50 U.S.C. §§ 1806(f), 1825(g).

As originally enacted, FISA required that a high-ranking official of the Executive Branch certify that "the purpose" of the FISA application was to obtain foreign intelligence information. In 2001, FISA was amended as part of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("PATRIOT Act"). Pub. L. No. 107-56, 115 Stat. 272 (2001). One change to FISA accomplished by the PATRIOT Act was the abrogation of the interpretation that the "primary purpose" of the

[2] An "aggrieved person" is defined as the target of electronic surveillance or "any other person whose communications or activities were subject to electronic surveillance," 50 U.S.C. § 1801(k), as well as "a person whose premises, property, information, or material is the target of physical search or any other person whose premises, property, information, or material was subject to physical search." 50 U.S.C. § 1821(2). As discussed *infra*, the defendant is an "aggrieved person" under FISA, and, as such, he has been provided notice of the Government's

requested FISA surveillance be the gathering of foreign intelligence information; instead, a high-ranking official of the Executive Branch is now required to certify that the acquisition of foreign intelligence information is "a significant purpose" of the requested surveillance. 50 U.S.C. § 1804(a)(6)(B). As discussed in detail in later sections of this Memorandum, the "significant purpose" standard is constitutional.

FISA authorizes the use in a criminal prosecution of information obtained or derived from any FISA-authorized electronic surveillance or physical search, provided that advance authorization is obtained from the Attorney General, *see* 50 U.S.C. §§ 1806(b), 1825(c), and that proper notice is given to the court and to each aggrieved person against whom the information is to be used, *see* 50 U.S.C. §§ 1806(c), (d), and 1825(d), (e). Upon receiving notice, an aggrieved person may then move to suppress the use of FISA-obtained or -derived information on two grounds: (1) that the information was unlawfully acquired under FISA; or (2) that the electronic surveillance or the physical search was not conducted in conformity with an order of authorization or approval. 50 U.S.C. §§ 1806(e), 1825(e).

[CLASSIFIED MATERIAL REDACTED]

B. THE FISA APPLICATION

[CLASSIFIED MATERIAL REDACTED]

An application to conduct electronic surveillance pursuant to FISA must contain, among other things: (1) the identity of the federal officer making the application; (2) the identity, if known, or a description of the specific target of the electronic surveillance; (3) a statement of the facts and circumstances supporting probable cause to believe that the target is a foreign

---

intent to use FISA-obtained or FISA-derived information against him at trial.

power or an agent of a foreign power, and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power; (4) a statement of the proposed minimization procedures to be followed; (5) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance; (6) a certification, discussed below, of a high-ranking official of the Executive Branch; (7) the manner or means by which the electronic surveillance will be effected and a statement whether physical entry is required to effect the electronic surveillance; (8) the facts concerning and the action taken on all previous FISA applications involving any of the persons, facilities, places, premises or property specified in the application; and (9) the proposed duration of the electronic surveillance. *See* 50 U.S.C. § 1804(a)(1)-(9).

An application to conduct a physical search pursuant to FISA must contain similar information as an application to conduct electronic surveillance. *See* 50 U.S.C. § 1823(a)(1)-(8). The primary difference is that an application to conduct a physical search must also contain a statement of the facts and circumstances justifying the applicant's belief that "the premises or property to be searched contains foreign intelligence information" and that "[each] premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from" an agent of a foreign power or a foreign power. *See* 50 U.S.C. §§ 1823(a)(3)(B), (C).

1. The Certification

An application to the FISC for a FISA order must include a certification from a high-ranking official of the Executive Branch with national security responsibilities:

> (A) that the certifying official deems the information sought to be foreign intelligence information;
> (B) that a significant purpose of the surveillance [or search] is to obtain foreign intelligence information;
> (C) that such information cannot reasonably be obtained by normal investigative techniques;
> (D) that designates the type of foreign intelligence information being sought according to the categories described in [50 U.S.C. § 1801(e)]; and
> (E) including a statement of the basis for the certification that – (i) the information sought is the type of foreign intelligence information designated; and (ii) such information cannot reasonably be obtained by normal investigative techniques.

50 U.S.C. § 1804(a)(6).[3]

2. Minimization Procedures

The Attorney General has adopted, and the FISC has approved, minimization procedures that regulate the acquisition, retention, and dissemination of non-publicly available information obtained through FISA collection concerning non-consenting U.S. persons, including persons who are not the targets of the FISA collection. *In re Sealed Case*, 310 F.3d 717, 728 n.16 (FISA Rev. Ct. 2002), *rev'd on other grounds*. FISA requires that such minimization procedures must be:

> [S]pecific procedures . . . that are reasonably designed in light of the purpose and technique of the particular surveillance [or physical search], to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

50 U.S.C. §§ 1801(h)(1), 1821(4)(A).

---

[3] The language quoted above describes the requirements for an application for authority to conduct electronic surveillance. The requirements for an application for authority to conduct a physical search are the same, except that subparagraph (E) reads, "includes a statement explaining the basis for the certifications required by subparagraphs (C) and (D)." 50 U.S.C.§

In addition, minimization procedures include "procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." 50 U.S.C. §§ 1801(h)(3), 1821(4)(C).

[CLASSIFIED MATERIAL REDACTED]

3. Attorney General's Approval

FISA further requires that the Attorney General, or his designee, as explained *supra*, approve each application for electronic surveillance or physical search and find that it satisfies the statutory requirements before it is presented to the FISC. 50 U.S.C. §§ 1804(a), 1823(a).

C. THE FISC'S ORDERS

Once approved by the Attorney General, each FISA application is submitted to the FISC and assigned to one of its judges. The FISC must enter an *ex parte* order[4] as requested, or modified by the judge approving the electronic surveillance or physical search upon finding, among other things, that: (1) the application has been made by a "Federal officer" and has been approved by the Attorney General; (2) there is probable cause to believe that the target of the surveillance or search is a foreign power or an agent of a foreign power, and each of the facilities or places at which electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power (or, in the case of a physical search, the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power); (3) the proposed minimization procedures meet

---

1823(a)(6).

[4] **[CLASSIFIED MATERIAL REDACTED]**

the requirements set forth in 50 U.S.C. § 1801(h) (or, in the case of a physical search, 50 U.S.C. § 1821(4)); and (4) the application contains all of the statements and certifications required by 50 U.S.C. § 1804 (or, in the case of a physical search, by 50 U.S.C. § 1823), and, if the target is a U.S. person, the certifications are not clearly erroneous. 50 U.S.C. §§ 1805(a), 1824(a).

FISA defines foreign powers to include "group[s] engaged in international terrorism or activities in preparation therefor." 50 U.S.C. § 1801(a)(4) (adopted by incorporation by 50 U.S.C. § 1821(1)). As it relates to U.S. persons, an "agent of a foreign power" includes any person who "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power," 50 U.S.C. § 1801(b)(2)(C) (adopted by incorporation by 50 U.S.C. § 1821(1)), as well as any person who "knowingly aids or abets any person in the conduct of," or "knowingly conspires with any person to engage in," the aforementioned conduct. 50 U.S.C. § 1801(b)(2)(E) (adopted by incorporation by 50 U.S.C. § 1821(1)).

FISA specifies that no U.S. person may be considered a foreign power or an agent of a foreign power solely on the basis of activities protected by the First Amendment. 50 U.S.C. §§ 1805(a)(2)(A), 1824(a)(2)(A). Although protected First Amendment activities cannot form the sole basis for FISA-authorized electronic surveillance or physical search, they may be considered by the FISC if there is other activity indicating that the target is an agent of a foreign power. In *United States v. Rosen*, the district court stated:

> Thus, while the statute is intended to avoid permitting electronic surveillance solely on the basis of First Amendment activities, it plainly allows a FISC judge to issue an order allowing surveillance or physical search if there is probable cause to believe that the target, even if engaged in First Amendment activities, may also be involved in unlawful clandestine intelligence activities, or in knowingly aiding

> and abetting such activities. In these circumstances, the fact that a target is also involved in protected First Amendment activities is no bar to electronic surveillance pursuant to FISA.

447 F. Supp. 2d 538, 549-50 (E.D. Va. 2006). Similarly, in *United States v. Rahman*, the court summarily rejected as "simply wrong" the defendant's argument that "no statements of his that are arguably protected by. . .the First Amendment could constitute evidence that he was an agent of a foreign power." 861 F. Supp. 247, 252 (S.D.N.Y. 1994), *aff'd*, 189 F.3d 88 (2d Cir. 1999) (citations omitted). Additionally, FISA provides that "[i]n determining whether or not probable cause exists . . . a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." 50 U.S.C. §§ 1805(b), 1824(b).

A FISC order itself authorizing electronic surveillance or physical search must specify the following: (1) the identity, or a description of, the target; (2) the nature and location of each facility or place at which the electronic surveillance will be directed, or of each of the premises or properties to be searched; (3) the type of information sought to be acquired and the type of communications or activities to be subjected to the electronic surveillance (or, in the case of a physical search, the type of information, material or property to be seized, altered, or reproduced); (4) the means by which electronic surveillance will be effected and whether physical entry will be used to effect the surveillance (or, in the case of a physical search, the manner in which the search is to be conducted and, when more than one search is authorized, the authorized scope of each and the minimization procedures applicable to information acquired by each); and (5) the period of time during which surveillance or searching is approved. 50 U.S.C. §§ 1805(c)(1), 1824(c)(2). The FISC also retains the authority to review, before the end of the authorized

period of surveillance or searching, compliance with the requisite minimization procedures. 50 U.S.C. §§ 1805(d)(3), 1824(d)(3).

Under FISA, electronic surveillance or a physical search targeting a U.S. person may be approved for ninety days or the period necessary to achieve its purpose, whichever is less. 50 U.S.C. §§ 1805(d)(1), 1824(d)(1). Extensions may be granted, but only upon the submission of another application in compliance with FISA. 50 U.S.C. §§ 1805(d)(2), 1824(d)(2).

III. DISTRICT COURT REVIEW OF FISC ORDERS

FISA contemplates the use in a criminal prosecution of information obtained or derived from FISA-authorized electronic surveillance or physical search, provided that advance authorization is obtained from the Attorney General, *see* 50 U.S.C. §§ 1801(h)(3), 1806(b), 1821(4)(C), 1825(c), and that proper notice is given to the court and to each "aggrieved person" against whom the information is to be used, *see* 50 U.S.C. §§ 1806(c), 1825(d). With respect to electronic surveillance, an aggrieved person is "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k). With respect to a physical search, an aggrieved person is "a person whose premises, property, information, or material is the target of physical search or any other person whose premises, property, information, or material was subject to physical search." *See* 50 U.S.C. § 1821(2).

FISA provides that a person against whom evidence obtained or derived from a FISA-authorized electronic surveillance or physical search to which he or she is an aggrieved person is to be used may move to suppress the evidence on two grounds: (1) that the information was unlawfully acquired; or (2) that the electronic surveillance or physical search was not

conducted in conformity with the FISC's order(s). 50 U.S.C. §§ 1806(e), 1825(f)(1). Upon receipt of such a motion, the U.S. District Court in which the evidence obtained or derived from FISA is to be used must determine whether the electronic surveillance or physical search was "lawfully authorized and conducted." 50 U.S.C. §§ 1806(f), 1825(g).

A. THE REVIEW IS TO BE CONDUCTED *IN CAMERA* AND *EX PARTE*

In assessing the legality of challenged FISA-authorized electronic surveillance or physical searches, the district court "shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance [or physical search] as may be necessary to determine whether the surveillance [or physical search] of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. §§ 1806(f), 1825(g).[5] On the filing of the Attorney General's affidavit or declaration, the court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to [electronic] surveillance *only where such disclosure is necessary* to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f) (emphasis added). In the case of a physical search, "only where such disclosure is necessary," the court may require the Attorney General to disclose to the aggrieved person a summary of such materials. 50 U.S.C. § 1825(g). The propriety of the disclosure of any FISA application or order to the defense cannot even be considered unless and until the district court has first concluded that it is unable to make an accurate determination of the legality of the collection after reviewing the

Government's submissions (and any supplemental pleadings that the district court may request) *in camera* and *ex parte*. *See United States v. El-Mezain,* No. 09-10560, 2011 WL 6058592, at *84 (5th Cir. 2011); *Abu-Jihaad*, 630 F.3d at 129; *United States v. Belfield,* 692 F.2d 141, 147 (D.C. Cir. 1982); *United States v. Kashmiri*, No. 09-CR-830-4, 2010 WL 4705159, at *3 (N.D. Ill. Nov. 10, 2010) ("A court has never permitted defense counsel to review FISA materials."); *United States v. Nicholson*, No. 09-CR-40-BR, 2010 WL 1641167, at *3 (D. Or. Apr. 21, 2010); *United States v. Islamic American Relief Agency,* No. 07-00087-CR-W-NKL, 2009 WL 5169536, at *3 (W.D. Mo. Dec. 21, 2009) ("*IARA*").

If the district court is able to make an accurate determination of the legality of the electronic surveillance and physical search based on its *in camera, ex parte* review of the materials submitted by the United States, then the court *may not* order disclosure of any of the FISA materials to the defense, unless otherwise required by due process. *See* 50 U.S.C. §§ 1806(g), 1825(h); *El-Mezain,* 2011 WL 6058592, at *84; *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984) (affirming district court's refusal to disclose FISA materials where court was able to determine legality of surveillance without disclosure to defense); *Kashmiri*, 2010 WL 4705159, at *2 ("If disclosure of the FISA materials is not necessary for the district court to make an accurate determination of the legality of the collection, disclosure *may not be ordered.*" (emphasis in original)); *United States v. Warsame*, 547 F. Supp. 2d 982, 987 (D. Minn. 2008) ("[t]he legislative history explains that such disclosure is 'necessary' only where the court's initial review indicates that the question of legality may be complicated" by factual misrepresentations, insufficient identification of the target, or failure to comply with the

[5] 50 U.S.C. 1825(g) refers to "any other provision of law" rather than "any other law."

minimization standards in the order). Likewise, if the court is able to determine the legality of the FISA collection, then a hearing is also unnecessary: "The demand for an adversary hearing must fall with the demand for disclosure of the *in camera* Exhibit. They are inextricably linked. [When] disclosure is not necessary, no purpose would be served by an evidentiary hearing." *Belfield*, 692 F.2d at 147.

Federal courts have consistently held that FISA anticipates that an *in camera, ex parte* process is to be the rule, with disclosure and an adversarial hearing being the exception, occurring only when necessary. *See Abu-Jihaad*, 630 F.3d at 129 ("disclosure of FISA materials is the exception and *ex parte, in camera* [review] is the rule.") (internal quotation marks omitted); *El-Mezain,* 2011 WL 6058592, at *85; *Belfield*, 692 F.2d 147; *United States v. Stewart*, 590 F.3d 93, 129 (2d Cir. 2009); *Duggan*, 743 F.2d at 78; *United States v. Spanjol*, 720 F. Supp. 2d 55, 59 (E.D. Pa. 1989), *aff'd* 958 F.2d 365 (3rd Cir. 1992). Indeed, no court has ever found it necessary to disclose FISA materials to the defendant to assist the court's determination of the lawfulness of either electronic surveillance or physical searches under FISA. *See Kashmiri*, 2010 WL 4705159, at *3; *United States v. Gowadia*, No. 05-00486, 2009 WL 1649714, at *2 (D. Haw. June 8, 2009); *United States v. Mubayyid*, 521 F. Supp. 2d 125, 130 (D. Mass. 2007) (collecting cases); *Rosen*, 447 F. Supp. 2d at 546 (same).

The underlying rationale for non-disclosure is clear: "Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to anyone not involved in the surveillance operation in question . . . ." *United States v. Ott*, 827 F.2d 473, 477 (9th. Cir. 1987). Confidentiality is critical to national security. "If potentially valuable intelligence sources"

believe that a United States intelligence agency "will be unable to maintain the confidentiality of its relationship to them," then those sources "could well refuse to supply information." *CIA v. Sims*, 471 U.S. 159, 175 (1985) (upholding CIA's refusal to disclose information pursuant to a Freedom of Information Act request). When a question is raised as to whether the disclosure of classified sources, methods, techniques, or information would harm the national security, courts have expressed a great reluctance to second-guess the considered judgment of Executive Branch officials charged with the responsibility of "weigh[ing] the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the . . . intelligence-gathering process." *Sims*, 471 U.S. at 180; *see also United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989) (reversing district court's order directing disclosures pursuant to Classified Information Procedures Act and noting "[t]hings that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods"); *Halperin v. CIA*, 629 F.2d 144, 150 (D.C. Cir. 1980) (affirming denial of FOIA request and noting that "each individual piece of intelligence information, much like a piece of a jigsaw puzzle, may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself").

As the D.C. Circuit explained in rejecting a constitutional challenge to FISA's *ex parte* procedures:

> Congress recognized the need for the Executive to engage in and employ the fruits of clandestine surveillance without being constantly hamstrung by disclosure requirements. The statute is meant to "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." In FISA the privacy rights of

> individuals are ensured not through mandatory disclosure, but through its provisions for in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which governs law-enforcement surveillance.

Belfield, 692 F.2d at 148 (footnotes and citations omitted).

In summary, FISA mandates a process by which the district court must conduct an *in camera, ex parte* review of FISA applications, orders, and related materials in order to determine whether challenged FISA collections were lawfully authorized and lawfully conducted, before the issue of possible disclosure to the defense even arises. In this case, the Attorney General has filed the required declaration invoking that procedure, and has declared that disclosure or an adversary hearing would harm national security.[6] Accordingly, an *in camera, ex parte* review by this Court is the appropriate method by which to determine whether the FISA collections were lawfully authorized and conducted pursuant to FISA.

B. THE DISTRICT COURT'S SUBSTANTIVE REVIEW

In evaluating the legality of the FISA collection, the district court's review should determine: (1) whether the certification submitted by the Executive Branch in support of a FISA application was properly made; (2) whether the application established the probable cause showing required by FISA; and (3) whether the collection was properly minimized. *See Abu-Jihaad*, 630 F.3d at 130-31. *See also* 50 U.S.C. §§ 1806(f), 1825(g).

---

[6] As previously discussed, the Attorney General's Declaration and Claim of Privilege is based on the classified Declaration of Ralph S. Boelter the Assistant Director of the FBI's Counterterrorism Division, submitted herewith as Sealed Exhibit 2 in the Sealed Appendix. In his Declaration, Assistant Director Boelter sets out in detail the specific harm to national security that would result from the disclosure of the FISA materials in this case.

Although federal courts are not in agreement as to whether the probable cause determinations of the FISC should be reviewed *de novo* or accorded due deference, the materials under review here clear the higher standard of *de novo* review. *See Abu-Jihaad*, 630 F.3d at 130 ("Although the established standard of judicial review applicable to FISA warrants is deferential, the government's detailed and complete submission in this case would easily allow it to clear a higher standard of review."). The Government respectfully submits that it is appropriate to accord due deference to the findings of the FISC, but notes that a number of courts, including *Warsame,* have declined to do so, citing the *ex parte* nature of the proceedings, and have instead reviewed the FISC's probable cause determination *de novo*. *Warsame,* 547 F. Supp. 2d at 990.[7] While decidedly in the minority, other courts, including the Second Circuit in *Abu-Jihaad*, have afforded due deference to the FISC. *See Abu-Jihaad*, 630 F.3d at 130; *accord United States v. Ahmed*, No. 06-147, 2009 U.S. Dist. LEXIS 120007, at *21-22 (N.D. Ga. Mar. 19, 2009) (FISC's "determination of probable cause should be given 'great deference' by the reviewing court") (citing *Illinois v. Gates*, 462 U.S. 213, 236 (1983)).

In the analogous area of criminal searches and surveillance, the law in the Eighth Circuit accords great deference to a magistrate judge's probable cause determinations. *See, e.g.,*

---

[7] *Accord Rosen*, 447 F. Supp. 2d at 545 (*citing United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004), *rev'd on other grounds*, 543 U.S. 1097 (2005), *op. reinstated in pertinent part*, 405 F.3d 1034 (4th Cir. 2005)); *Kashmiri,* 2010 WL 4705159, at *1 (*citing Hammoud*, 381 F.3d at 332); *Nicholson*, 2010 WL 1641167, at *5 (*citing Rosen*, 447 F. Supp. 2d at 447). However, *Hammoud* says nothing about the proper scope of the district court's review of the FISC's probable cause determinations. Rather, it states, without discussion, that the court of appeals conducted a *de novo* review. *See Hammoud,* 381 F.3d at 332 (*citing United States v. Squillacote*, 221 F.3d 542, 554 (4th Cir. 2000) (same)). Thus, the *de novo* review referred to in *Hammoud* may be nothing more than the Court's reference to the accepted standard of review of a trial court's probable cause determination on appeal from denial of a motion to suppress. *See*

United States v. Kattaria, 553 F.3d 1171, 1175 (8th Cir. 2009). It would be consistent for a court that is reviewing FISA-authorized searches and surveillance to adopt the same posture it would when reviewing the probable cause determination of a criminal search warrant issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure. *See Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *21-22 (according FISC's probable cause determinations the same deference as magistrate's criminal probable cause determination).[8] In that context, the "duty of a reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed" at the time of the application. *Kattaria*, 553 F.3d at 1175 (*citing Gates*, 462 U.S. at 238-39).

This Court confronted the issue recently in three cases and ruled that, even applying a *de novo*-review standard, there was sufficient probable cause. *See United States v. Mohamed*, No. 09-CR-00352 (MJD/SER), Docket No. 99, Memorandum Opinion and Order at 13 (D. Minn. June 27, 2011); *United States v. Ali*, No. 10-CR-00187 (MJD/FLN), Docket No. 100, Memorandum Opinion and Order at 14 (D. Minn. June 27, 2011); *United States v. Ahmed*, No. 11-CR-00191 (MJD/FLN), Docket No. 59, Memorandum Opinion and Order at 12 (D. Minn. Jan. 18, 2012).

[CLASSIFIED MATERIAL REDACTED]

United States v. Blake, 571 F.3d 331, 338 (4th Cir. 2009).

[8] *Ahmed* is not alone in analogizing FISA orders to search warrants. *See, e.g., United States v. Cavanagh*, 807 F.2d 713, 790 (9th Cir. 1987) (concluding that FISA order can be considered a warrant since it is issued by a detached judicial officer and is based on a reasonable showing of probable cause); *In re Sealed Case*, 310 F.3d at 74 (declining to decide whether a FISA order constitutes a warrant, but noting "that to the extent a FISA order comes close to meeting Title III, that certainly bears on its reasonableness under the Fourth Amendment"); *but see Warsame*, 547 F. Supp. 2d at 992 n.10 (noting that the need for foreign intelligence justifies

1. FISA Certifications Are Subject to Minimal Scrutiny

A certification submitted in support of a FISA application should be "subjected to only minimal scrutiny by the courts," *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987), and is "presumed valid." *Duggan*, 743 F.2d at 77 & n.6 (citing *Franks* 438 U.S. at 171); *Nicholson*, 2010 WL 1641167, at *5; *Warsame*, 547 F. Supp. 2d at 990 (affording a "presumption of validity" to the certifications); *accord United States v. Campa*, 529 F.3d 980, 993 (11th Cir. 2008). When a FISA application is presented to the FISC, "[t]he FISA Judge, in reviewing the application, is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information." *Duggan*, 743 F.2d at 77. Likewise, Congress intended that the reviewing district court should "have no greater authority to second-guess the executive branch's certifications than has the FISA judge." *Id.; see also In re Grand Jury Proceedings of the Special April 2002 Grand Jury,* 347 F.3d 197, 204-05 (7th Cir. 2003); *Badia,* 827 F.2d at 1463; *Rahman,* 861 F. Supp. at 250; *IARA*, 2009 WL 5169536, at *4; *Kashmiri*, 2010 WL 4705159, at *1.

The district court's review should determine whether the certification was made in accordance with FISA's requirements. *See United States v. Ahmed*, No. 06-147, 2009 U.S. Dist. LEXIS 120007, at *20 (N.D. Ga. Mar. 19, 2009) ("the [c]ourt is not to second-guess whether the certifications were correct, but merely to ensure they were properly made"). Where the target of the FISA is a U.S. person, the district court must also ensure that each certification is not "clearly erroneous." *Campa*, 529 F.3d at 994; *Duggan*, 743 F.2d at 77; *Kashmiri*, 2010 WL 4705159, at *2; *Warsame*, 547 F. Supp. 2d at 990. A certification is clearly erroneous only when "the

---

an exception to the warrant requirement).

reviewing court on the entire evidence is left with the definite and firm conviction that a mistake has been committed." *IARA*, 2009 WL 5169536, at *4 (*citing United States v. U.S. Gypsum Co.*, 333 U.S. 364, 395 (1948)); *see also United States v. Berger*, 553 F.3d 1107, 1109 (8th Cir. 2009).

2. FISA's Probable Cause Standard Differs from the Probable Cause Standard in the Criminal Context

As discussed above, FISA requires a finding of probable cause that the target is a foreign power or an agent of a foreign power and that each of the facilities at which electronic surveillance was being directed was being used, or was about to be used, by a foreign power or an agent of a foreign power, and that the property to be searched was or was about to be owned, used, possessed by, or in transit to or from, by a foreign power or an agent of a foreign power. 50 U.S.C. §§ 1805(a)(2), 1824(a)(2); *United States v. Cavanagh,* 807 F.2d 787, 789 (9th Cir. 1987); *IARA,* 2009 WL 5169536, at *5. This standard is intentionally different from and "less stringent than" that applicable in the ordinary criminal context, reflecting "a constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to obtain foreign intelligence information." *Duggan*, 743 F.2d at 73. It is this standard, not the standard applicable to a criminal search warrant, that this Court must apply. *See, e.g.*, *El-Mezain*, 2011 WL 6058592, at *82 ("[t]his probable cause standard is different from the standard in the typical criminal case because, rather than focusing on probable cause to believe that a person has committed a crime, the FISA standard focuses on the status of the target as a foreign power or an agent of a foreign power"); *Abu-Jihaad*, 630 F.3d at 130-31; *Cavanagh,* 807 F.2d at 790 (citing *United States v. United States District Court (Keith),* 407 U.S. 297, 322

(1972)). This "different, and arguably lower, probable cause standard . . . reflects the purpose for which FISA search orders are issued." *Ahmed,* 2009 U.S. Dist. LEXIS 120007, at *22.

3. Minimization

If a reviewing court is satisfied that the electronic surveillance or physical search was properly certified and lawfully authorized pursuant to FISA, it must then examine whether the electronic surveillance or physical search was lawfully conducted. *See* 50 U.S.C. §§ 1806(e)(2), 1825(f)(1)(B). In order to examine whether the electronic surveillance or physical search was lawfully conducted, the reviewing court must determine whether the Government followed the relevant minimization procedures to appropriately minimize the information acquired pursuant to FISA.

[CLASSIFIED MATERIAL REDACTED]

FISA's legislative history and the applicable case law demonstrate that the definitions of "minimization procedures" and "foreign intelligence information" were intended to take into account the realities of collecting foreign intelligence because the activities of persons engaged in clandestine intelligence gathering or international terrorism are often not obvious on their face. *See Rahman*, 861 F. Supp. at 252-53. The degree to which information is required to be minimized varies somewhat given the specifics of a particular investigation, such that less minimization at acquisition is justified when "the investigation is focusing on what is thought to be a widespread conspiracy" and more extensive surveillance is necessary "to determine the precise scope of the enterprise." *In re Sealed Case*, 310 F.3d at 741; *see also United States v. Bin Laden*, 126 F. Supp. 2d 264, 286 (S.D. N.Y. 2000) ("more extensive monitoring and greater leeway in minimization efforts are permitted in a case like this given the world-wide, covert and

diffuse nature of the international terrorist group(s) targeted" (internal quotation marks omitted)). Furthermore, the activities of foreign powers and their agents are often not obvious from an initial or cursory overhear of conversations. To the contrary, agents of foreign powers frequently engage in coded communications, compartmentalized operations, the use of false identities and other practices designed to conceal the breadth and aim of their operations, organization, activities and plans. *See, e.g., United States v. Salameh*, 152 F.3d 88, 154 (2d Cir. 1998) (noting that two conspirators involved in the 1993 bombing of the World Trade Center in New York referred to the bomb plot as the "study" and to terrorist materials as "university papers"). As one court explained, "[i]nnocuous-sounding conversations may in fact be signals of important activity; information on its face innocent when analyzed or considered with other information may become critical." *Kevork*, 634 F. Supp. at 1017 (quoting H.R. Rep. No. 95-1283,55, 95th Cong., 2d Sess., Pt. 1 (1978) (hereinafter "House Report")); *see also Hammoud*, 381 F.3d at 334 (citing *Salameh*, 152 F.3d at 154); *In re Sealed Case*, 310 F.3d at 740-41; *United States v. Thomson*, 752 F. Supp. 75, 81 (W.D.N.Y. 1990) (noting that it is permissible to retain and disseminate "bits and pieces" of information until the information's "full significance becomes apparent") (citing House Report, part 1, at 58); *Bin Laden*, 126 F. Supp. 2d at 286. Likewise, "individual items of information, not apparently significant when taken in isolation, may become highly significant when considered together over time." *Rahman*, 861 F. Supp. at 252-53 (citing House Report, part 1, at 55, 59). The Government must be given flexibility where the conversations are carried out in a foreign language. *Mubayyid*, 521 F. Supp. 2d at 134; *Rahman*, 861 F. Supp. at 252. As a result, "courts have construed 'foreign intelligence

information' broadly and sensibly allowed the government some latitude in its determination of what is foreign intelligence information." *Rosen*, 447 F. Supp. 2d at 551.

The nature of the foreign intelligence information sought also impacts implementation of the minimization procedures at the retention and dissemination stages. There is a legitimate need to conduct a thorough post-acquisition review of FISA information that involves a U.S. person who is acting as an agent of a foreign power. Congress explained:

> It is "necessary" to identify anyone working with him in this network, feeding him information, or to whom he reports. Therefore, it is necessary to acquire, retain and disseminate information concerning all his contacts and acquaintances and his movements. Among his contacts and acquaintances, however, there are likely to be a large number of innocent persons. Yet, information concerning these persons must be retained at least until it is determined that they are not involved in the clandestine intelligence activities and may have to be disseminated in order to determine their innocence.

House Report, part 1, at 58. Indeed, at least one court has cautioned that, when a U.S. person communicates with an agent of a foreign power, the Government would be "remiss in meeting its foreign counterintelligence responsibilities" if it did not thoroughly "investigate such contacts and gather information to determine the nature of those activities." *Thomson*, 752 F. Supp. at 82.

Congress also recognized that agents of a foreign power are often very sophisticated and skilled at hiding their activities. *Cf. Thomson*, 752 F. Supp. at 81 (quoting House Report part 1, at 58). Accordingly, to pursue leads, Congress intended that the Government be given "a significant degree of latitude" with respect to the "retention of information and the dissemination of information between and among counterintelligence components of the Government." *Cf. Thomson*, 752 F. Supp. at 81 (quoting House Report part 1, at 58).

In light of these realities, Congress recognized that "no electronic surveillance can be so conducted that innocent conversations can be totally eliminated." *See* S. Rep. No. 95-701, 95th Cong., 2d Sess., 39 (quoting *Keith.*, 407 U.S. at 323) (1978) ("Senate Report"). The Fourth Circuit reached the same conclusion in *Hammoud*, stating that the "mere fact that innocent conversations were recorded, without more, does not establish that the government failed to appropriately minimize surveillance." 381 F.3d at 334. Accordingly, in reviewing the adequacy of minimization efforts, the test to be applied is neither whether innocent conversations were intercepted, nor whether mistakes were made with respect to particular communications. Rather, as the Supreme Court stated in the context of Title III surveillance, there should be an "objective assessment of the [agents'] actions in light of the facts and circumstances confronting [them] at the time." *Scott v. United States*, 436 U.S. 128, 136 (1978). The test of compliance is whether a good-faith effort to minimize was made. *Hammoud*, 381 F.3d at 334 ("[t]he minimization requirement obligates the Government to make a good faith effort to minimize the acquisition and retention of irrelevant information"); *see also* at 39-40 (stating that the court's role is to determine whether "on the whole, the agents have shown a high regard for the right of privacy and have done all they reasonably could do to avoid unnecessary intrusion"); *IARA*, 2009 WL 5169536, at *6 (quoting Senate Report at 39-40); *Mubayyid*, 521 F. Supp. 2d at 135.

Moreover, as noted above, FISA expressly states that the Government is not required to minimize information that is "evidence of a crime," whether or not it is also foreign intelligence information. 50 U.S.C. §§ 1801(h)(3), 1821(4)(c); *see also United States v. Isa*, 923 F.2d 1300, 1304 (8th Cir. 1991) (noting that "[t]here is no requirement that the 'crime' be related to foreign

intelligence"). As a result, to the extent that certain communications of a U.S. person may be evidence of a crime or otherwise may establish an element of a substantive or conspiratorial offense, such communications need not be minimized. *See Isa*, 923 F.2d at 1305.

Even assuming, *arguendo*, that certain communications were not properly minimized, suppression is not the appropriate remedy with respect to the communications that met the standard. *Cf. United States v. Falcone*, 364 F. Supp. 877, 886-87 (D.N.J. 1973), *aff'd*, 500 F.2d 1401 (3d Cir. 1974) (Title III). As discussed above, absent evidence that "on the whole" there has been a "complete" disregard for the minimization procedures, the fact that a court might conclude that some communications should have been minimized does not affect the admissibility of items properly acquired and retained. Indeed, Congress specifically intended that the only evidence that should be suppressed is the "evidence which was obtained unlawfully." House Report at 93. FISA's legislative history reflects that Congress intended only a limited sanction for errors of minimization:

> As the language of the bill makes clear, only that evidence which was obtained unlawfully or derived from information obtained unlawfully would be suppressed. If, for example, some information should have been minimized but was not, only that information should be suppressed; the other information obtained lawfully should not be suppressed.

Id.; *see also Falcone*, 364 F. Supp. at 886-87.

4. <u>There Should Neither Be Disclosure Nor Suppression</u>

If a reviewing court determines that a FISA collection was both lawfully authorized and conducted, it must deny any request for disclosure of the FISA materials and for the suppression of evidence obtained or derived from the FISA collection "except to the extent that due process requires discovery or disclosure." 50 U.S.C. §§ 1806(g), 1825(h).

In view of the classified submissions to the Court, the Attorney General's Declaration and Claim of Privilege, which is supported by a highly detailed and specific Declaration of a high-ranking FBI official, and in light of the applicable law, the Government respectfully submits that there is no basis upon which to order an unprecedented disclosure of the FISA materials or the suppression of any of the FISA-obtained or –derived information that the Government intends to offer into evidence at trial. Accordingly, upon completing its review, the Court should deny the defendant's FISA Motion.

IV. THE COURT SHOULD REJECT THE DEFENDANT'S CONSTITUTIONAL CHALLENGES TO FISA

[CLASSIFIED MATERIAL REDACTED]

The defendant also states that he seeks disclosure of FISA materials under the First, Fourth, Fifth, and Sixth Amendments of the U.S. Constitution. (*See* Def. FISA Mot. Supp. at 1.) Later, he argues that the Court should order disclosure of the FISA applications, affidavits, certifications, opinions, and related to materials to the defense to allow the defense to assist the Court with its analyis. (*See* Def. FISA Mot. Supp. at 13-15.) These arguments have no merit. Below the Government responds to the defendant's arguments that disclosure of the FISA materials is mandated by the Fifth and Sixth Amendments of the U.S. Constitution. In addressing the facts constituting probable cause, *infra*, the Government responds to the argument that it improperly relied on First Amendment activities to establish probable cause.

A. THE PROBABLE CAUSE STANDARD OF FISA COMPLIES WITH THE FOURTH AMENDMENT'S REASONABLENESS REQUIREMENT

The probable cause threshold which the Government must satisfy before receiving authorization to conduct electronic surveillance or a physical search under FISA complies with the Fourth Amendment's reasonableness standard. The argument that FISA's different, and arguably lower, probable cause standard violates the Fourth Amendment's reasonableness requirement has been uniformly rejected by federal courts. *See, e.g., Abu-Jihaad,* 630 F.3d at 120 (listing sixteen cases that have ruled FISA does not violate the Fourth Amendment).

The Supreme Court has stated that "[d]ifferent standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of the Government for intelligence information and the protected rights of our citizens." *Keith*, 407 U.S. at 322-23 (recognizing that domestic security surveillance "may involve different policy and practical considerations than the surveillance of 'ordinary crime'"). In *Keith,* the Supreme Court acknowledged that: (1) the "focus of . . . surveillance [in domestic security investigations] may be less precise than that directed against more conventional types of crime"; (2) unlike ordinary criminal investigations, "[t]he gathering of security intelligence is often long range and involves the interrelation of various sources and types of information"; and (3) the "exact targets of such surveillance may be more difficult to identify" than in surveillance operations of ordinary crimes under Title III. *Id.* Although *Keith* was decided before FISA's enactment and addressed purely domestic security surveillance, the rationale underlying *Keith* applies *a fortiori* to foreign intelligence surveillance, where the Government's interest, at least from a national security perspective, would typically be more pronounced.

FISA was enacted partly in response to *Keith.* In constructing FISA's framework, Congress addressed *Keith's* question of whether departures from traditional Fourth Amendment

procedures "are reasonable, both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens," and "concluded that such departures are reasonable." *See* Senate Report at 11. Similarly, many courts – including the FISC of Review – have relied on *Keith* in holding that FISA collection conducted pursuant to a FISC order is reasonable under the Fourth Amendment. *See In re Sealed Case,* 310 F.3d at 738, 746 (finding that while many of FISA's requirements differ from those in Title III, few of those differences have constitutional relevance); *Duggan,* 743 F.2d at 74 (holding that FISA does not violate the Fourth Amendment); *see also United States v. Ning Wen,* 477 F.3d 896, 898 (7th Cir. 2006) (holding that FISA is constitutional despite using "a definition of 'probable cause' that does not depend on whether a domestic crime has been committed"); *United States v. Damrah,* 412 F.3d 618, 625 (6th Cir. 2005) (denying the defendant's claim that FISA's procedures violate the Fourth Amendment); *United States v. Pelton,* 835 F.2d 1067, 1075 (4th Cir. 1987) (finding FISA's procedures compatible with the Fourth Amendment); *Cavanagh,* 807 F.2d at 790-91 (holding that FISA satisfies the Fourth Amendment requirements of probable cause and particularity); *Warsame*, 547 F. Supp. 2d at 993-94 (holding that FISA's probable cause and particularity requirements satisfy the reasonableness requirement of the Fourth Amendment); *Mubayyid,* 521 F. Supp. 2d at 135-41 (rejecting claim that FISA violates the Fourth Amendment's judicial review, probable cause, notice, and particularity requirements); *United States v. Falvey,* 540 F. Supp. 1306, 1311-14 (E.D. N.Y. 1982) (finding that FISA procedures satisfy the Fourth Amendment's warrant requirement).

The Eighth Circuit rejected a Fourth Amendment challenge to FISA in *Isa.* 923 F.2d at 1304. There, the defendant was charged in state court with first degree murder. *Id.* The

defendant challenged the use of the inculpatory telephone conversations collected through the authorities granted by FISC orders targeting the defendant at his residence, asserting that FISA's probable cause standard was insufficient to warrant the "highly intrusive nature" of the surveillance of his residence. *Id.* The Eighth Circuit affirmed the district court's conclusion that the FISA collection did not violate the Fourth Amendment, and rejected the defendant's challenge to FISA's lower probable cause threshold. *Id.*

B. THE SIGNIFICANT PURPOSE STANDARD DOES NOT VIOLATE THE FOURTH AMENDMENT

In his FISA Motion, the defendant challenges FISA's significant purpose standard, which replaced the primary purpose standard. The primary purpose test was originally derived from consideration of warrantless searches that were conducted pursuant to the Executive's Article II foreign-affairs powers prior to the enactment of FISA. *Abu-Jihaad*, 630 F.3d at 121. In that context, warrantless surveillance could be conducted as an exception to the Fourth Amendment, and would therefore be limited to the scope of the Constitution's grant of authority to the Executive to conduct foreign affairs. *See United States v. Truong Dihn Hung*, 629 F.2d 908 (4th Cir. 1980) (holding warrantless foreign intelligence surveillance constitutional with respect to a foreign power, its agents or collaborators when conducted primarily for foreign intelligence reasons). Once enacted, FISA originally required that a high-ranking official of the Executive Branch certify that "the purpose" of the FISA application was to obtain foreign intelligence information. Prior to the PATRIOT Act's amendment of FISA, several courts imported the "primary purpose" test from warrantless surveillance into the statutory interpretation of FISA's certification requirement. *See Duggan*, 743 F.2d at 77; *Pelton*, 835

F.2d at 1075-76; *Badia*, 827 F.2d at 1463; *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991).[9] None of those cases held that the primary purpose test was constitutionally mandated,[10] as the Second Circuit pointed out in *Abu-Jihaad*:

> [W]e note that when, in *Duggan*, we construed FISA's original reference to electronic surveillance for "the purpose" of obtaining foreign intelligence information, as a "requirement that foreign intelligence information be the *primary* objective . . ." we were identifying Congress's intent in enacting FISA, not a constitutional mandate. . . . In short, nothing in *Duggan* erected a constitutional bar to Congress reconsidering and reframing the purpose requirement of FISA.

630 F.3d at 123-24 (citations omitted).

In 2001, FISA was amended by the PATRIOT Act, which *inter alia*, deleted "the purpose" language, and instead substituted the requirement that the official certify that "a significant purpose" of the requested surveillance is to obtain foreign intelligence information. 50 U.S.C. § 1804(a)(6)(B). The factors driving Congress's amendment included two considerations that emerged from years of experience with the primary purpose requirement: "(1) if intelligence and law enforcement officials coordinate efforts in pursuing national security inquiries, it can be difficult, if not impossible, to identify whether their 'primary' purpose is to obtain foreign intelligence information or evidence of a crime; and (2) the segregation of intelligence and law enforcement officials to ensure the executive's ability to certify a 'primary' foreign-intelligence-gathering purpose can compromise national security." *Abu-Jihaad*, 630

---

[9] In *Johnson*, the First Circuit actually construed the purpose requirement in the negative, holding that "the investigation of criminal activity cannot be the primary purpose" of FISA surveillance. 952 F.2d at 572.

[10] The Ninth Circuit took a contrary view and hesitated to define FISA's purpose requirement "to draw too fine a distinction between criminal and intelligence investigations," because by definition international terrorism requires the investigation of some activities that also

F.3d at 124. The Amendments to FISA following the terrorist attacks of September 11, 2001, deleted the primary purpose test and thereby eliminated a perceived obstacle to joint efforts by law enforcement and intelligence officials to conduct electronic surveillance or physical searches where the subject is potentially a source of valuable intelligence and also a target of a criminal investigation.

With the exception of the now-vacated and legally null *Mayfield v. United States*, 504 F. Supp. 2d 1023 (D. Or. 2007), *vacated*, 599 F. 3d 964 (9th Cir. 2010), *cert. denied*, 131 S. Ct. 503 (2010),[11] upon which the defendant heavily relies, each court to have considered the PATRIOT Act amendment setting forth the significant purpose test has held the test is constitutional. *See Abu-Jihaad*, 630 F.3d at 128 ("FISA's 'significant purpose' requirement . . . is sufficient to ensure that the executive may only use FISA to obtain a warrant when it is in good faith pursuing foreign intelligence gathering [and the] fact that the government may also be pursuing other purposes, including gathering evidence for criminal prosecution, compels no different conclusion."); *Damrah*, 412 F.3d at 625; *In re Sealed Case*, 310 F.3d at 746; *Mubayyid*, 521 F. Supp. 2d at 139; *United States v. Marzook*, 435 F. Supp. 2d 778, 786 (N.D. Ill. 2006); *United States v. Benkahla*, 437 F. Supp. 2d 541, 554 (E.D. Va. 2006); *Mubayyid*, 521 F. Supp. 2d at 139-40. In *Warsame*, the Court did not reach the issue, concluding that the "significant

---

constitute crimes. *United States v. Sarkissian*, 841 F.2d 959, 965 (9th Cir. 1988).

[11] FISA's "significant purpose" standard was held unconstitutional in *Mayfield*, a civil case, which no other court followed and the United States Court of Appeals for the Ninth Circuit eventually vacated on the ground that the plaintiff lacked standing. *See Mayfield v. United States*, 588 F.3d 1252 (9th Cir. 2009). And, as is the case for the lower court's decision in *Mayfield*, when a judgment is vacated by a higher court "it deprives the [lower] court's opinion of precedential effect." *Los Angeles County v. Davis*, 440 U.S. 625, 634 n.6 (1979). Moreover, the district court's rational in *Mayfield* was specifically rejected in *Kashmiri*, 2010

purpose" requirement was not unconstitutional as it applied to FISA orders in that case, because the court satisfied itself that "the primary purpose of the FISA surveillance and searches was to gather foreign intelligence, and was not to prosecute [the defendant] for criminal activity." 547 F. Supp. 2d at 997 ("Ultimately, however, the Court need not decide the issue [of whether the significant purpose test is constitutional].")

Indeed, when confronted with the same argument recently, this Court ruled as follows: "Based on the applicable law, the Court is satisfied that FISA's significant purpose requirement is consistent with the Fourth Amendment's protections against unreasonable searches and seizures." *Mohamed*, No. 09-CR-352 (MJD/FLN), Memorandum Opinion and Order at 16; *Ali*, No. 10-CR-00187 (MJD/FLN), Memorandum Opinion and Order at 14-15; *Ahmed*, No. 11-CR-191 (MJD/FLN), Memoradum Opinion and Order at 14. Here, this Court should reach the same conclusion, finding that FISA's probable cause standards are constitutional.

C. CHALLENGES TO FISA'S *IN CAMERA, EX PARTE* REVIEW

1. The Court's *In Camera* and *Ex Parte* Review Satisfies the Fifth Amendment's Due Process Clause

The constitutionality of FISA's *in camera, ex parte* review provisions has been affirmed by every Federal court that has considered the matter. *See, e.g., Abu-Jihaad,* 630 F.3d at 117, 129; *Spanjol*, 720 F. Supp. at 58; *Damrah*, 412 F.3d at 624 ("FISA's requirement that the district court conduct an *ex parte*, *in camera* review of FISA materials does not deprive a defendant of due process."); *Ott*, 827 F.2d at 476-77 (holding that FISA's review procedures do

---

WL 4705159, at *6.

not deprive a defendant of due process); *Gowadia*, 2009 WL 1649714, at *2; *Belfield*, 692 F.2d at 148-49; *Warsame*, 547 F. Supp. 2d at 989 ("disclosure of FISA materials to [the defendant] is not necessary for an accurate determination of the legality of the surveillance, and not necessary to adequately safeguard [the defendant's] due process rights."); *Benkahla*, 437 F. Supp. 2d at 554; *ACLU Found. of S. Cal. v. Barr*, 952 F.2d 457, 465 (D.C. Cir. 1991); *United States v. Megahey*, 553 F. Supp. 1180, 1194 (E.D.N.Y. 1982) ("*ex parte, in camera* procedures provided in 50 U.S.C. § 1806(f) are constitutionally sufficient to determine the lawfulness of the electronic surveillance at issue while safeguarding defendants' fourth amendment rights"); *Falvey*, 540 F. Supp. at 1315-16 (a "massive body of pre-FISA case law of the Supreme Court, [the Second] Circuit and others" supports the conclusion that the legality of electronic surveillance should be determined on an *in camera, ex parte* basis); *Nicholson*, 2010 WL 1641167, at *3; *IARA*, 2009 WL 5169536, at *6-7.

Moreover, this Court recently came to the same conclusion, ruling that it was satisfied that its review of the FISA materials permitted the Court to adequately assess the legality of the surveillance, and that due process did not counsel otherwise. *Mohamed*, No. 09-CR-352 (MJD/FLN), Memorandum Opinion and Order at 15; *Ali*, No. 10-CR-00187 (MJD/FLN), Memorandum Opinion and Order at 16-17; *Ahmed*, No. 11-CR-191 (MJD/FLN), Memoradum Opinion and Order at 14. Here, too, the Court should also reject the defendant's argument and rule that the Due Process Clause of the Fifth Amendment does not require disclosure of the FISA materials.

2. The Court's *In Camera* and *Ex Parte* Review Does Not Offend the Defendant's Sixth Amendment Rights to Counsel and Confrontation

To the extent that the defendant is positing that his Sixth Amendment rights to counsel and to confrontation are violated because an *ex parte* review compromises his attorney's ability to advocate on his behalf, his arguments are without merit.[12] The Eighth Circuit specifically has rejected a constitutional challenge to FISA's *in camera, ex parte* review provision based on an argument that *ex parte, in camera* review violates the Sixth Amendment right to confrontation. *See Isa*, 923 F.2d at 1306-07 (finding that FISA's *in camera, ex parte* review procedures do not violate the Sixth Amendment right of confrontation). There, the court ruled that the right of confrontation is "not absolute" and may bow to accommodate legitimate interests in the criminal trial process. *Id.* The court held that, given the substantial interests at stake and the protections provided, the Sixth Amendment rights of the appellant were not violated. *Id.*

A similar Sixth Amendment argument was advanced unsuccessfully in *Warsame*. 547 F. Supp. 2d at 988 n.4 (finding argument "without merit" and citing to *United States v. Nicholson*, 955 F. Supp. 588, 592 (E.D. Va. 1997)). Other courts have also consistently rejected the Sixth Amendment argument. *See Belfield*, 692 F.2d at 148 (rejecting Sixth Amendment challenge); *Megahey*, 553 F. Supp. at 1193 (rejecting Sixth Amendment challenge); *Benkhala*, 437 F. Supp. 2d at 554 (rejecting Sixth Amendment right to counsel challenge); *Nicholson*, 955 F. Supp. 592 & n.11 (rejecting Sixth Amendment right to counsel challenge); *Falvey*, 540 F. Supp.

[12] On the first page of his FISA Motion, the defendant relies upon the Sixth Amendment to the U.S. Constitution in asking the Court to review all of the FISA applications at issue, disclose such applications to the defense, and suppress any and all related FISA-obtained or –derived evidence. (Def. FISA Mot. at 1.) Thereafter, the defendant neither cites to nor relies upon either the Sixth Amendment. The Government will address the defendant's reliance upon the Sixth Amendment as being directed toward the statutorily mandated *in camera, ex parte* review of the FISA applications at issue.

at 1315-16 (rejecting First, Fifth and Sixth Amendment challenges and noting that a "massive body of pre-FISA case law of the Supreme Court, [the Second] Circuit and others" supports the conclusion that the legality of electronic surveillance should be determined on an *in camera, ex parte* basis).

Indeed, as a district court recently stated, "Every court that has considered FISA's constitutionality has upheld the statute from challenges under the Fourth, Fifth, and Sixth Amendments." *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *30 (order denying defendants' motion to disclose and suppress FISA materials).

V. THE FISA COLLECTION WAS BOTH LAWFULLY AUTHORIZED AND CONDUCTED

The defendant's FISA Motion contends that suppression of any FISA-obtained or -derived information, and disclosure of the FISA materials, is necessary because: (1) probable cause to demonstrate that any FISA targets were agents of a foreign power is lacking; (2) any FISA applications do not show that a significant purpose of the collection was to obtain foreign intelligence; (3) the certifications were clearly erroneous, and the Government might have violated the authorized time periods for collection; and (4) any applications contain false statements in violation of *Franks*. (Def. FISA Mot. Sup., at 12-19.)

[CLASSIFIED MATERIAL REDACTED]

A. THE FISA COLLECTION WAS LAWFULLY AUTHORIZED

[CLASSIFIED MATERIAL REDACTED]

1. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. **Foreign Intelligence Information**

[CLASSIFIED MATERIAL REDACTED]

b. **"A Significant Purpose"**

[CLASSIFIED MATERIAL REDACTED]

c. **Information Not Reasonably Obtainable Through Normal Investigative Techniques**

[CLASSIFIED MATERIAL REDACTED]

d. **Argument**

[CLASSIFIED MATERIAL REDACTED]

2. **All Statutory Requirements Were Met**

[CLASSIFIED MATERIAL REDACTED]

3. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

(1) [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

(2) [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

(3) [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

(4) [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

(5) Argument

[CLASSIFIED MATERIAL REDACTED]

b. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

(1) [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

(A) [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

(B) [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

(C) Argument

[CLASSIFIED MATERIAL REDACTED]

(2) [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

(A) [CLASSIFIED MATERIAL REDACTED]

1. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

2. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

3. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

4. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

5. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

(B) [CLASSIFIED MATERIAL REDACTED]

1. [CLASSIFIED MATERIAL REDACTED]

A. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

B. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

2. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

B. THE FISA COLLECTION WAS LAWFULLY CONDUCTED

This Court's *in camera, ex parte* review of the FISA materials will demonstrate not only that the FISA collection was lawfully authorized, but also that they were lawfully conducted. That is, the information collected pursuant to the FISA authorities at issue herein ("the FISA information") was acquired, retained, and disseminated by the FBI in accordance with FISA's minimization requirements, and the implementing SMPs adopted by the Attorney General and approved by the FISC.

[CLASSIFIED MATERIAL REDACTED]

Based upon this information, we respectfully submit that the Government lawfully conducted the FISA collection at issue herein. Consequently, for the reasons stated above, the Court should find that the FISA collection at issue in this case were lawfully conducted under the minimization procedures approved by the FISC and applicable to the FISA collection at issue herein.

VI. ANALYSIS OF THE DEFENDANT'S SPECIFIC ARGUMENTS

The Attorney General has filed a declaration in this case stating that disclosure or an adversary hearing would harm the national security of the United States. Therefore, FISA mandates that this Court conduct an *in camera, ex parte* review of the challenged FISA materials to determine whether the collection at issue were both lawfully authorized and conducted. In conducting that review, the Court may disclose the FISA materials "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance [or search]." *See* 50 U.S.C. §§ 1806(f), 1825(g). As discussed above, Congress, in enacting FISA's procedures for *in camera, ex parte* judicial review, has balanced and accommodated the competing interests of the Government and criminal defendants, and has articulated the proper standard for disclosure; that is, only where the Court finds that disclosure is necessary to the Court's accurate determination of the legality of the FISA collection. *See id.* The Court will be able to render a determination based on its *in camera, ex parte* review, and the defendant has failed to present any colorable basis for supplanting Congress' reasoned judgment with a different proposed standard of review.

The Court can make this determination without disclosing the classified and highly sensitive FISA materials to the defendant. Every court that has addressed a motion to disclose

FISA materials has denied the motion and determined the legality of the FISA collection based on an *in camera, ex parte* review. *See, e.g., El-Mezain,* 2011 WL 6058592, at *84 (quoting the district court's statement that no court has ever ordered disclosure); *Abu-Jihaad,* 630 F.3d at 129; *United States v. Dumesi,* 424 F.3d 566, 578-79 (7th Cir. 2005); *In re Grand Jury Proceedings,* 347 F.3d at 203 (noting that no court has ever ordered disclosure of FISA materials); *Johnson,* 952 F.2d at 571-73; *Badia,* 827 F.2d at 1463-64; *Duggan,* 743 F.2d 59, 78 (2d Cir. 1984); *United States v. Amawi,* 531 F. Supp. 2d 832, 837 (N.D. Ohio 2008); *Mubayyid,* 521 F. Supp. 2d at 130; *Rosen,* 447 F. Supp. 2d at 546; *Nicholson,* 955 F. Supp. at 588, 592 & n.11 ("[T]his court knows of no instance in which a court has required an adversary hearing or disclosure in determining the legality of a FISA surveillance."); *Thomson,* 752 F. Supp. at 79; *Spanjol,* 720 F. Supp. at 59 (*in camera, ex parte* procedure has been "uniformly followed by all Courts which have reviewed the legality of electronic surveillances authorized by the [FISC]"); *Gowadia,* 2009 WL 1649714, at *2 ("[t]o date, no court has held that disclosure of the FISA application papers was necessary in order to determine the lawfulness of a search authorized under FISA"); *Nicholson,* 2010 WL 1641167, at *4 ("After an *in-camera* review, the court 'has the discretion to disclose portions of the documents, under appropriate protective orders, *only if [the court] decides that such disclosure is necessary to make an accurate determination of the legality of the surveillance.* '") (emphasis in original); *Kashmiri,* 2010 WL 4705159, at *6.

The Government respectfully submits that there is nothing extraordinary about this case that would prompt the Court to be the first to order the disclosure of highly sensitive and classified FISA materials. Disclosure is simply not necessary in order for the Court to determine the legality of the FISA collection at issue. Every federal court that has been asked to

determine the legality of a FISA-authorized collection has been able to do so *in camera* and *ex parte* and without the assistance of defense counsel. In addition, the FISA materials at issue here are organized and readily understandable, and an overview of them is presented herein as a frame of reference. *Cf. Kevork*, 634 F. Supp. at 1008. In addition, the FISA materials and other exhibits contain ample information from which the Court can make an accurate determination of the legality of the FISA collection; indeed, they are "relatively straightforward and not complex." *See, e.g., Abu-Jihaad*, 630 F.3d at 129 (upholding district court's *in camera, ex parte* review where FISA dockets were "relatively straightforward and not complex"); *Belfield*, 692 F.2d at 147 ("[t]he determination of legality in this case is not complex"); *Warsame*, 547 F. Supp. 2d at 987 (finding that "issues presented by the FISA applications are straightforward and uncontroversial"). Thus, there is no basis on which to disclose the FISA materials to the defendant. *See, e.g., Thomson*, 752 F. Supp. at 79 (finding no disclosure of FISA dockets warranted under Section 1806(f) where issues were "not so complex that the participation of the defendant [was] required to accurately determine the legality of the surveillance at issue"). The Government respectfully submits that this Court, much like the aforementioned courts, will be able to determine the legality of the FISA collection based on its *in camera, ex parte* review of the materials submitted in the Government's Sealed Appendix.

[CLASSIFIED MATERIAL REDACTED]

As stated above, in his FISA Motion, the defendant argues for relief on the following grounds: (1) that FISA is unconstitutional as written and as applied to the FISA collection at issue; (2) that the FISA applications at issue fail to make the requisite showings to permit collection under FISA, in that they do not demonstrate that a significant purpose of the collection

at issue was to obtain foreign intelligence and because probable cause was lacking to authorize such collection; (3) that the certifications required by 18 U.S.C. § 1804(a)(6) were clearly erroneous; and (4) that the applications at issue contain false statements in violation of *Franks*. (*See generally* Def. FISA Mot. Supp.) As explained above, none of these grounds have merit.

[CLASSIFIED MATERIAL REDACTED]

Nor does reliance by the defense on the U.S. Constitution or the requirements of due process require any suppression of FISA-obtained evidence or disclosure of the FISA materials to the defense. Courts faced with the issue have uniformly held that the probable cause requirements of FISA comport with the requirements of the Fourth Amendment to the United States Constitution, *see, e.g., Isa,* 923 F.2d at 1304, and that FISA's provisions for *in camera* and *ex parte* review comport with the due process requirements of the United States Constitution. *See, e.g., Spanjol*, 720 F. Supp. at 58-59; *United States v. Butenko*, 494 F.2d 593, 607 (3d Cir.), *cert denied sub nom, Ivanov v. United States*, 419 U.S. 881 (1974); *Damrah*, 412 F.3d at 624; *Warsame*, 547 F. Supp. 2d at 988-89. Indeed, as a district court recently stated, "Every court that has considered FISA's constitutionality has upheld the statute from challenges under the Fourth, Fifth, and Sixth Amendments." *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *30 (order denying defendants' motion to disclose and suppress FISA materials). The defendant advances no argument to justify any deviation from the well-established precedent of *ex parte* and *in camera* review.

[CLASSIFIED MATERIAL REDACTED]

The defendant also contends that the Court should set a hearing pursuant to *Franks*, 438. U.S. at 154, arguing that such a hearing should be set because the defendant is unable to

access the FISA applications at issue. (Def. FISA Mot. at 17-19.) The standard under *Franks* warrants the opposite result, however. To merit an evidentiary hearing under *Franks,* a defendant must first make a "concrete and substantial preliminary showing" that: (1) the affiant deliberately or recklessly included false statements, or failed to include material information, in the affidavit; and (2) the misrepresentation was essential to the finding of probable cause. *Franks*, 438. U.S. at 155-56; *United States v. Colkley*, 899 F.2d 297, 301 (4th Cir. 1990). Failure of the defendant "to satisfy either of these two prongs proves fatal to a *Franks* hearing." *Kashmiri*, 2010 U.S. Dist. 2010 WL 4705159, at *6. *See also Mubayyid*, 521 F. Supp. 2d at 130-31. The defendant has not made a showing through the identification of any factual errors in any FISA application that would undercut a finding of probable cause. His reliance on a speculative possibility of error, and commentary in legal precedent regarding matters wholly unrelated to the instant FISA collection, are insufficient bases either for ordering disclosure of any FISA application at issue or for setting a *Franks* hearing. A defendant's "attack must be more than conclusory and must be supported by more than a mere desire to cross-examine." *Franks*, 438 U.S. at 171. *See also Mubayyid*, 521 F. Supp. 2d at 130-31; *Kashmiri*, 2010 U.S. Dist. LEXIS 119470, at *16 ("Without producing the requisite offer of proof of impropriety in the FISA application, however, this argument is merely conclusory, and equates to an improper direct attack on the FISA procedures"). Rather, a defendant must submit allegations of deliberate falsehood or of reckless disregard for the truth, accompanied by an offer of proof. *Franks*, 438 U.S. at 171. Allegations of negligence or innocent mistake are insufficient, *id.*, as are allegations of insignificant or immaterial misrepresentations or omissions. *Colkley*, 899 F.2d at 301-02. The *Franks* threshold is not met even by an offer proof of an impropriety that

might have affected the outcome of the probable cause determination, but rather requires one that was "necessary to the finding of probable cause." *Id.* Indeed, even if a defendant offers sufficient proof to show that an affidavit involved false statements or omissions, a hearing should not be held if the affidavit would still provide probable cause with the allegedly false material eliminated, or the allegedly omitted information included. *Franks*, 438 U.S. at 171; *Colkley*, 899 F.2d at 300; *United States v. Ketzeback*, 358 F.3d 987, 990 (8th Cir. 2004); *United States v. Martin*, 615 F.2d 318, 328 (5th Cir. 1980).

In this case, the defendant has not alleged any reason to believe that any FISA application contains any falsehoods or omissions, a showing required by *Franks*. Nor can the defendant's lack of access to any FISA application or order form a substitute basis for the requisite showing. Despite the quandary defense counsel inevitably face when notified that FISA-obtained or -derived evidence will be used against a defendant, Congress mandated, and the courts have recognized, that this quandary does not justify the disclosure of FISA materials:

> We appreciate the difficulties of appellants' counsel in this case. They must argue that the determination of legality is so complex that an adversary hearing with full access to relevant materials is necessary. But without access to relevant materials their claim of complexity can be given no concreteness. It is pure assertion.
>
> Congress was also aware of these difficulties. But it chose to resolve them through means other than mandatory disclosure. In FISA Congress has made a thoroughly reasonable attempt to balance the competing concerns of individual privacy and foreign intelligence . . . . Appellants are understandably reluctant to be excluded from the process whereby the legality of a surveillance by which they were incidentally affected is judged. But it cannot be said that this exclusion rises to the level of a constitutional violation.

Belfield, 692 F.2d at 148. *See also Mubayyid*, 521 F. Supp. 2d at 131 (quoting *Belfield*).

Further, as the court in *Kashmiri* stated:

> Nevertheless, to challenge the veracity of the FISA application, Defendant must offer substantial proof that the FISC relied on an intentional or reckless misrepresentation by the government to grant the FISA order. The quest to satisfy the *Franks* requirement might feel like a wild-goose chase, as Defendant lacks access to the materials that would provide this proof. This perceived practical impossibility to obtain a hearing, however, does not constitute a legal impossibility.

2010 U.S. Dist. 2010 WL 4705159, at * 6.

If a defendant could force disclosure of FISA materials or obtain an adversarial hearing merely by speculating that there *might* be a *Franks* violation somewhere in an application, the disclosure of FISA materials or adversarial hearings would be the rule and not the exception. Such a result would violate Congress' clear intent that FISA material should be reviewed *in camera* and *ex parte*, and in a manner consistent with the realities of intelligence needs and investigative techniques. In keeping with the well-established principle in the search warrant context that a defendant may only obtain a *Franks* hearing after making a "concrete and substantial preliminary showing," the defendant should be required to make such a showing before any disclosure is ordered or an adversarial hearing on *Franks* grounds can be contemplated. *Accord Kashmiri*, 2010 U.S. Dist. 2010 WL 4705159, at *6 (the Defendant "has not made any showing – let alone a substantial one – that an Executive Branch officer knowingly and intentionally, or recklessly, included a false statement in the FISA application [and w]ithout such a showing, he is foreclosed from obtaining a hearing"); *Duggan*, 743 F.2d at 77 n.6.[13]

[13] Several courts have rejected defense attempts to force a *Franks* hearing challenging the validity of FISA orders when the defense could offer no evidence to support their claims that the underlying applications were deficient. *See Abu-Jihaad*, 531 F. Supp. 2d at 311 (noting defense could "only speculate" about the FISA applications' contents); *United States v. Hassoun*,

For the reasons discussed above, we therefore respectfully submit that the FISA collection at issue were lawfully authorized and conducted, that the Court can make such a finding without the disclosure of the FISA materials, and that discovery or disclosure to the defense is not required by due process or *Brady*. Therefore, neither suppression of any FISA-obtained or -derived evidence nor disclosure of any FISA materials to the defense is warranted, and the Court must deny the defendant's FISA Motion. *See* 50 U.S.C. §§1806(g), 1825(h).

[CLASSIFIED MATERIAL REDACTED]

No. 04-60001-CR, 2007 WL 1068127, *4 (S.D. Fla. 2007) (denying request for a *Franks* hearing to challenge FISA applications where defendants' allegations were "purely speculative"); *Mubayyid*, 521 F. Supp. 2d at 130-31 (denying defendants' request for a *Franks* hearing to challenge FISA applications); *Kashmiri*, 2010 U.S. Dist. 2010 WL 4705159, at * 6 (denying defendant's request for a *Franks* hearing and noting that the court "has already undertaken a process akin to a *Franks* hearing through its *ex parte*, *in camera* review").

VII. CONCLUSION

[CLASSIFIED MATERIAL REDACTED]

Dated:

Respectfully submitted,

B. TODD JONES
United States Attorney

For: _____
JOHN DOCHERTY
CHARLES J. KOVATS, JR.
Assistant United States Attorneys

By: _____
WILLIAM M. NARUS
Trial Attorney
U.S. Department of Justice